UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

In the Matter of the Search of:	)	
	)	**Case No:** 2:23-mj-689
Information, including location data,	)	
associated with the Google Email address and account	)	**Magistrate Judge:** Vascura
treasuretaylor0256@gmail.com that is stored at	)	
premises controlled by Google LLC.	)	**UNDER SEAL**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Josh Saltar ("your affiant"), a Special Agent (SA) with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

I. EDUCATION, TRAINING AND EXPERIENCE

1. I am a Special Agent (SA) with the Federal Bureau of Investigations (FBI) and have been since October 2014. I am currently assigned to the Child Exploitation and Human Trafficking Task Force, Cincinnati Division, Columbus Resident Agency. I am primarily responsible for investigating internet crimes against children, including child pornography offenses and the online exploitation of children.
2. During my career as a SA, I have participated in various investigations involving computer-related offenses and have executed numerous search warrants, including those involving searches and seizures of computers, digital media, software, and electronically stored information. I have worked with multiple international law enforcement agencies around the world, focusing on cyber-terrorism and terrorist financing through computer intrusions. I have also assisted on various cases and violations, ranging from violent crimes against children and white collar to healthcare fraud, counterintelligence, and counterterrorism. As part of my duties as a Special Agent, I investigate criminal violations relating to child exploitation and sex trafficking of a minor, in violation of 18 U.S.C. §§ 1591.
3. Prior to joining the FBI, I spent four years working as a civilian Intelligence Specialist for the U.S. Air Force at the National Air and Space Intelligence Center located at the Wright-

Patterson Air Force Base, under both the cyber and counterspace squadrons, performing classified intel and reverse engineering duties. During my employment, I have received numerous forensic trainings with the both the Department of Defense and Department of Justice, as well as from private sector security conferences. I have received multiple certifications in Windows, mobile, and memory forensics, as well as incident response and penetration testing, and am certified by the Department of Justice as a Digital Extraction Technician. I received my B.A. from Anderson University in computer science, with a focus on programming, artificial intelligence, and machine learning.

4. As a SA with the FBI, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

5. I make this affidavit in support of an application for a search warrant for information associated with a certain Google account that is stored at premises owned, maintained, controlled, or operated by Google, LLC ("Google"), an electronic communications company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in **Attachment A**. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government records and other information in its possession, including the content of communications, pertaining to the subscriber or customer associated to the Google account **treasuretaylor0256@gmail.com** (hereinafter identified as the **SUBJECT ACCOUNT**).
6. The **SUBJECT ACCOUNT** to be searched are more particularly described in Attachment A, for the items specified in Attachment B, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 1591– sex trafficking of a minor. I am requesting authority to search the **SUBJECT ACCOUNT**, wherein the items specified in **Attachment B** may be found, and to seize all items listed in **Attachment B** as instrumentalities, fruits, and evidence of crime.

7. The facts set forth below are based upon my knowledge, experience, observations, and investigation, as well as the knowledge, experience, investigative reports, and information provided to me by other law enforcement agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every known fact to me relating to the investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1591– sex trafficking of a minor, are presently located in the **SUBJECT ACCOUNTS.** I have not omitted any facts that would negate probable cause.

III. APPLICABLE STATUTES AND DEFINITIONS

8. Title 18 United States Code, Section 1591 makes it a federal crime to knowingly recruit, harbor, entice, transport, provide, obtain, advertise, maintain, patronize, or solicit a person under the age of 18, knowing, or in reckless disregard of the fact that the person will be caused to engage in a commercial sex act.
9. The term "minor", as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as "any person under the age of eighteen years."
10. The term "computer"[1] is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
11. The terms "records", "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (such as writings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (such as printing or typing) or electrical, electronic or magnetic form (such as any and all digital

[1] The term "computer" is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

12. "Internet Service Providers" (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
13. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

IV. BACKGROUND INFORMATION REGARDING GOOGLE, GMAIL AND TECHNOLOGY

14. Google, LLC provides its subscribers internet-based accounts that allow them to send, receive, and store e-mails online. Google accounts are typically identified by a single username, which serves as the subscriber's default e-mail address, but which can also function as a subscriber's username for other Google services, such as instant messages and remote photo or file storage.
15. Based on my training and experience, I know that Google allows subscribers to obtain accounts by registering on Google's website. During the registration process, Google asks subscribers to create a username and password, and to provide basic personal information such as a name, an alternate e-mail address for backup purposes, a phone number, and, in some cases, a means of payment. Google typically does not verify subscriber names. However, Google does verify the e-mail address or phone number provided.
16. Once a subscriber has registered an account, Google provides e-mail services that typically include folders such as an "inbox" and a "sent mail" folder, as well as electronic address books or contact lists, and all of those folders are linked to the subscriber's username. Google subscribers can also use that same username or account in connection with other services provided by Google.
17. Notably, Google, LLC also provides "cloud" storage services. Account holder/users can utilize this service, which is called "Google Drive," to store pictures, videos, and other

electronic files remotely and without taking up memory space on their personal computer, smart phone, and physical storage media.

18. In general, user-generated content (such as e-mail) that is written using, stored on, sent from, or sent to a Google account can be permanently stored in connection with that account, unless the subscriber deletes the material. For example, if the subscriber does not delete an e-mail, the e-mail can remain on Google servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to exist on Google's servers for a certain period of time.

19. These services may include electronic communication services such as Google Voice (voice calls, voicemail, and SMS text messaging), Hangouts (instant messaging and video chats), Google+ (social networking), Google Groups (group discussions), Google Photos (photo sharing), and YouTube (video sharing); web browsing and search tools such as Google Search (internet searches), Web History (bookmarks and recorded browsing history), and Google Chrome (web browser); online productivity tools such as Google Calendar, Google Contacts, Google Docs (word processing), Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools (text translation); online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries); Pixel Phone (services which support a Google smartphone); and Google Play (which allow users to purchase and download digital content, e.g., applications).

20. Thus, a subscriber's Google account can be used not only for e-mail but also for other types of electronic communication, including instant messaging and photo and video sharing; voice calls, video chats, SMS text messaging; and social networking. Depending on user settings, user-generated content derived from many of these services is normally stored on Google's servers until deleted by the subscriber. Similar to e-mails, such user-generated content can remain on Google's servers indefinitely if not deleted by the subscriber, and even after being deleted, it may continue to be available on Google's servers for a certain period of time. Furthermore, a Google subscriber can store contacts, calendar data, images, videos, notes, documents, bookmarks, web searches, browsing history, and various other types of information on Google's servers.

21. Based on my training and experience, I know that evidence of who controlled, used, and/or created a Google account may be found within such computer files and other information created or stored by the Google subscriber. Based on my training and experience, I know that the types of data discussed above can include records and communications that constitute evidence of criminal activity.

22. Based on my training and experience, I know that providers such as Google also collect and maintain information about their subscribers, including information about their use of Google services. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. Providers such as Google also commonly have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with other logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which devices were used to access the relevant account. Also, providers such as Google typically collect and maintain location data related to subscriber's use of Google services, including data derived from IP addresses and/or Global Positioning System ("GPS") data.

23. Based on my training and experience, I know that providers such as Google also collect information relating to the devices used to access a subscriber's account – such as laptop or desktop computers, cell phones, and tablet computers. Such devices can be identified in various ways. For example, some identifiers are assigned to a device by the manufacturer and relate to the specific machine or "hardware," some identifiers are assigned by a telephone carrier concerning a particular user account for cellular data or voice services, and some identifiers are actually assigned by Google in order to track what devices are using Google's accounts and services. Examples of these identifiers include unique application number, hardware model, operating system version, Global Unique Identifier ("GUID"), device serial number, mobile network information, telephone number, Media Access Control ("MAC") address, and International Mobile Equipment Identity ("IMEI").

24. Based on my training and experience, I know that such identifiers may constitute evidence of the crimes under investigation because they can be used (a) to find other Google accounts created or accessed by the same device and likely belonging to the same user, (b) to find other types of accounts linked to the same device and user, and (c) to determine whether a particular device recovered during course of the investigation was used to access the Google account.
25. In addition, I know that Google maintains records that can link different Google accounts to one another, by virtue of common identifiers, such as common e-mail addresses, common telephone numbers, common device identifiers, common 7 computer cookies, and common names or addresses, that can show a single person, or single group of persons, used multiple Google accounts. Based on my training and experience, I also know that evidence concerning the identity of such linked accounts can be useful evidence in identifying the person or persons who have used a particular Google account.
26. Based on my training and experience, I know that subscribers can communicate directly with Google about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers such as Google typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.
27. In summary, based on my training and experience in this context, I believe that the servers of Google are likely to contain user-generated content such as stored electronic communications (including retrieved and unretrieved e-mail for Google subscribers), as well as Google-generated information about its subscribers and their use of Google services and other online services. In my training and experience, all of that information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In fact, even if subscribers provide Google with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities.

28. As explained above, information stored in connection with a Google account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element of the offense, or, alternatively, to exclude the innocent from further suspicion. From my training and experience, I know that the information stored in connection with a Google account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, e-mail communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by Google can show how and when the account was accessed or used. For example, providers such as Google typically log the IP addresses from which users access the account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the Google account access and use relating to the criminal activity under investigation. This geographic and timeline information may tend to either inculpate or exculpate the person who controlled, used, and/or created the account. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via e-mail). Finally, stored electronic data may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information in the Google account may indicate its user's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

V. INVESTIGATION AND PROBABLE CAUSE

29. On July 31, 2020, Columbus Division of Police (CPD) received a call from Witness One, a family member of the three minor victims identified in this case – approximately 13-year-old Minor Victim One (hereinafter MV1), approxiamtely12-year-old Minor Victim Two (hereinafter MV2), and approximately 7-year-old Minor Victim Three (hereinafter MV3). In the call, Witness One indicated that MV2 had been sexually assaulted. CPD conducted

an interview with MV2 that same day and MV2 informed law enforcement that approximately six months ago, Anthony **SIMS** talked her into smoking marijuana and getting high. At the time, **SIMS** was living with her, Witness One, MV1, and MV3. After MV2 got high on the marijuana, **SIMS** fondled MV2's breasts and vagina. Over the next four to five months, **SIMS** would encourage MV2 to drink alcohol or smoke marijuana and would then sexually assault MV2, to include penetrating MV2's vagina with his fingers and eventually his penis. MV2 went on to inform CPD that it would typically happen on the brown couch in the living room of the residence they shared. MV2 stated that **SIMS** raped her approximately 40-50 times throughout the six-month time frame, and at times would hold MV2's arms down or hold her in place as he sexually assaulted her. Additionally, MV2 reported that **SIMS** would force MV2 to undress and take nude photos of MV2 on a bronzed colored Motorola phone. **SIMS** would force MV2 to pose in different sexual positions and wear lingerie for some of the pictures.

30. Also on July 31, 2020, CPD conducted an interview with MV1 who also resided with **SIMS** during the same time period that MV2 did as well. MV1 informed CPD that **SIMS** convinced her to smoke marijuana with him. Once MV1 was high, **SIMS** began to penetrate MV1's vagina with his penis. On one occasion when this was occurring, they heard Witness One arrive home from work and **SIMS** stopped. According to MV1, **SIMS** told her not to tell anyone since no one would believe her. MV1 stated that **SIMS** vaginally penetrated her approximately five times, all when Witness One was at work and after getting MV1 drunk or high. According to MV1, **SIMS** would hold her arms down when he penetrated her vaginally and would also force MV1 to undress. When MV1 was nude, **SIMS** would take photos of her and made her pose with stuffed animals or pillows. MV1 informed law enforcement that **SIMS** sold the photos of her that he took and bought her a new phone with the money he made off of her.

31. In further investigation of **SIMS,** law enforcement learned that a registered sex offender with convictions out of Michigan. More specifically, **SIMS** was convicted on or about February 13, 1991 of violations of Michigan Penal Code section 750.520C1A - Criminal Sexual Conduct – Second Degree (Person Under 13) and 750.520B1A - Criminal Sexual Conduct – First Degree (Person Under 13).

32. Witness One took MV1 and MV2 for sexual assault kits and medical follow-ups on or about August 4, 2020. Law enforcement learned that MV2 tested positive for chlamydia and gonorrhea.
33. On August 10, 2020, law enforcement spoke with **SIMS** telephonically. **SIMS** denied any allegations of touching either MV1 or MV2. According to **SIMS,** Witness One was asking MV1 and MV2 to make up the story up and stated that they were lying, but that MV1 and MV2 were good kids. During the same conversation, **SIMS** informed law enforcement that he had recently been treated for gonorrhea. Legal process was served to the hospital **SIMS** he was treated at to verify this information.
34. On August 11, 2020, a forensic interview was conducted with MV3 who also resided with Witness One, MV1, MV2, and **SIMS.** MV3 stated that **SIMS** would "kiss her on her private part or lips" and that he would "lick her on her private parts". MV3 went on to say that **SIMS** laid her across the bed of Witness One and got on top of her so she couldn't move. According to MV3, **SIMS** would pull her clothes up onto her stomach and pull her underwear down and "kiss her on the skin of her private part".
35. On August 12, 2020, law enforcement received the medical records for **SIMS** and learned that on July 7, 2020, SIMS had tested positive for chlamydia and gonorrhea, the same two STD's MV2 had tested positive for on August 4, 2020.
36. On August 24, 2020, an arrest warrant was issued for **SIMS** out of Franklin County, Ohio for three counts of Ohio Revised Code 2907.02 ORC violations of Rape, a felony in the first degree.
37. On September 18, 2020, **SIMS** was arrested in Chicago, Illinois on the arrest warrant and extradited back to Columbus, Ohio. At the time he was arrested in Chicago, he was in possession of a Samsung Galaxy A20 that was inventoried with the Chicago Police Evidence Recovery and Property Section (ERPS). **SIMS** is currently incarcerated in Franklin County pending trial on these charges.
38. On November 3, 2022, law enforcement received a call from Witness One again. Witness One learned from a school counselor of MV1 that MV1 made new recent disclosures about what **SIMS** had done to her. More specifically, MV1 disclosed to a school counselor that in addition to being raped by **SIMS**, **SIMS** would get MV1 drunk or high and take her to various hotels to force her to have sex with men who paid **SIMS.** MV1 stated she was

forced to have sex with approximately 50 different men, and that it would mostly happen on weekends when she was out of school.

39. On November 17, 2022, a forensic interview with conducted with MV1. During the interview, MV1 recalled a specific incident in which she was violently raped by an unknown individual after **SIMS** transported her to an unknown hotel to meet the unknown male. Afterward, the unknown male left the hotel room and MV1 was left there and noticed her vagina was bleeding. When she informed **SIMS** about the incident and injuries, **SIMS** told MV1 "that will probably happen again". During the interview, MV1 stated **SIMS** did all the communications on his cell phone with various messaging apps. MV1 believed **SIMS** had two cell phones, both Android phones. She went on to say he used one phone for taking nude photos of her and setting up the meetings with men at hotels, and the other phone to mainly stay in touch with family.
40. As the investigation of **SIMS** continued and expanded, law enforcement obtained the Samsung Galaxy A20 cell phone belonging to **SIMS** from ERPS in Chicago, Illinois. On November 21, 2022, a search warrant was obtained in Franklin County for that device.
41. Upon the forensic extraction of the device being completed, a review of the analysis revealed that the Google account antoniopickett99@gmail.com was associated to the device during the forensic review. On February 16, 2023, legal process was served to Google for information pertaining to that account.
42. As the review of the forensic extraction of the Samsung Galaxy continued, law enforcement identified multiple images of MV1 and MV2 wearing lingerie or fully nude, and posed on a bed with their breasts, vaginas, or both exposed. Images were also recovered which depicted MV1 and MV2 engaged in masturbation. Based on these images, law enforcement reached out to your affiant with the FBI's Child Exploitation and Human Trafficking (CEHT) Task Force and requested assistance in forensic review of the cell phone and possible adoption of the case as it related to the production of child sexual abuse material. On February 22, 2023, your affiant opened an investigation.
43. Upon reviewing the forensic extraction of **SIMS** Samsung Galaxy cell phone, your affiant identified approximately 238 images depicting MV1 in various poses that were sexual in nature, both partially clothed as well as fully nude. One image depicted MV1 wearing a light blue lace top pulled down to expose her breast. In the image, MV1 was fully nude

from the waist down with her vagina exposed to the camera while laying on a bed. A second image depicted MV1 standing fully nude next to a bed with a bright pink star patterned comforter.

44. In continued forensic review of the cell phone, your affiant identified approximately 58 images depicting MV2 in various sexual poses, both partially clothed as well as fully nude. One image depicted MV2 wearing a black lace top and fully nude from the waist down. In the image, MV2's legs are spread open, and her nude vagina exposed to the camera while she was sitting on a bed. A second image depicted MV2 fully nude with her legs spread open and her vagina exposed to the camera while laying down on a bed with a spotted blue patterned comforter.
45. Your affiant identified an additional image from the device that depicted **SIMS** laying on a bed with the same spotted blue patterned comforter as the one depicted in the image described above of MV2. Metadata associated with the image identified the following information:
    - Capture Date: 4/28/2019 5:24:23 AM
    - Latitude/Longitude: 39.972775 / -82.962281

    That latitude and longitude resolved to 292 Johnson Street, Columbus, Ohio 43203, which was the same address provided by Witness One where Witness One and all three Minor Victims resided with **SIMS** in 2019.
46. Your affiant also identified the Samsung Galaxy phone had a phone number attributed to it which was noted as (317) 480-0021.
47. Your affiant was also provided a copy of the Google search warrant for the Google account antoniopickett99@gmail.com which was attributed to the phone as noted above. In review of those returns, your affiant identified location history dating back to 2019. Based off the information provided by MV1 to the school counselor, your affiant reviewed all location data available from July 2019 through August 2020, with a focus on locations traveled over weekends. Your affiant identified numerous hotels that were visited within Columbus, Ohio and the surrounding area over multiple weekends.
48. On December 7, 2023, your affiant met with MV1 and asked MV1 if she had a Google account back in 2019 that was tied to her cellular phone, and MV1 confirmed she did. MV1 then gave your affiant permission to review her Google account's location data in order to

be able to identify possible hotel locations that were visited. Your affiant explained to MV1 that he would like to compare that information to the hotels visited identified in the antoniopickett99@gmail.com account location data. MV1 provided her Google account as **treasuretaylor0256@gmail.com,** the **SUBJECT ACCOUNT**. Your affiant explained to MV1 that he would need to get a search warrant in order for Google to provide the necessary data, to which MV1 stated that she understood.

49. Based on the information that has been gathered to date by your affiant and other law enforcement entities, including interviews with the identified victims noted above, law enforcement reports, subpoena requests and returns, your affiant has reason to believe that the individual utilizing the **SUBJECT ACCOUNT,** most likely MV1, was utilizing the **SUBJECT ACCOUNT** on a cellular device that also contained evidence of sex trafficking of a minor. Therefore, it is likely that the **SUBJECT ACCOUNT** also contains items which constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 1591– sex trafficking of a minor. Your affiant respectfully requests that this Court issue a search warrant for the account described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

VI. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

50. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(l)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment.

VII. CONCLUSION

51. Based on the aforementioned factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. §§ 1591– sex trafficking of a minor, is located in the content of the **SUBJECT ACCOUNT** described in Attachment A. Your affiant respectfully requests that the Court issue a search warrant authorizing the search of the

locations identified in Attachment A and the seizure of the items described in Attachment B.

52. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Furthermore, because the warrant will be served on Google LLC, who will then compile the requested records at a time convenient to it, there is reasonable cause to permit the execution of the warrant at any time in the day or night.

Josh Saltar
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 11th day of December, 2023.

Chelsey M. Vascura, United States Magistrate Judge
United States District Court
Southern District of Ohio

ATTACHMENT A
PROPERTY TO BE SEARCHED

This warrant applies to information associated with the following Google email account (previously identified as the **SUBJECT ACCOUNT**), which is stored and maintained at premises owned, maintained, controlled, or operated by Google, LLC, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California:

1.) **treasuretaylor0256@gmail.com**

ATTACHMENT B
PROPERTY TO BE SEIZED

I. Information to be disclosed by Google:

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, LLC, including any records that have been deleted but are still available to Google, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose said information, logs, location data, and other information constituting fruits, contraband, instrumentalities, evidence, or proof of state of mind, with respect to violations of 18 U.S.C. §§ 1591 - sex trafficking of a minor, with regard to each account or identifier for the **SUBJECT ACCOUNT** listed in Attachment A for the time period of February 2019-September 2020:

The following information about the customers or subscribers of the **SUBJECT ACCOUNT**:

1. Names (including subscriber names, usernames, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
3. Local and long-distance telephone connection records;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
5. Length of service (including start date) and types of service utilized;
6. Telephone or instrument numbers (including MAC addresses);
7. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
8. Means and source of payment for such service (including any credit card or bank account number) and billing records.

2. All accounts linked to the **SUBJECT ACCOUNT** (including where linked by machine cookie or other cookie, creation or login Internet Protocol ("IP") address, recovery email or phone number, AOL account ID, Android ID, Google ID, SMS, Apple ID, or otherwise ("Linked Accounts").
3. Any and all push notification tokens for the **SUBJECT ACCOUNT** and SMS recovery numbers;

4. Any Google Wallet Data to include Google Play service data;
5. A complete listing of all enabled Google Services;
6. Android devices associated with or registered to the account;
7. Any additional user accounts associated with these Android devices;
8. All records and other information (not including the contents of communications) relating to the **SUBJECT ACCOUNT**, including:
    1. Records of user activity for each connection made to or from the **SUBJECT ACCOUNT** including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; usernames; connectivity information to include account change history and password change history; full history of all logins to include cookie logins; raw AMT logs for account access; and source and destination Internet Protocol addresses; and
    2. Information about each communication sent or received by the **SUBJECT ACCOUNT**, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers); and
    3. All IP logs and other documents showing the IP address, date, and time of each login and logout to the **SUBJECT ACCOUNT**, including "Active Sessions" information (all stored active sessions, including date, time, device, IP address, machine cookie and browser information); and
    4. Accounts to which any Linked Accounts are themselves linked, other than the **SUBJECT ACCOUNT**, by cookie, including machine cookie; and
    5. Language settings information; and
    6. All advertising data related to the **SUBJECT ACCOUNT** including but not limited to, information regarding unique advertising IDs associated with the Target Account(s), application IDs, UDIDs, payment information (including, but not limited to, full credit card numbers and expiration dates and PayPal accounts), and Pixel information; and
    7. User agent information and device ID information, including all devices used to access the **SUBJECT ACCOUNT** and Android IDs

9. Any and all cookies associated with or used by any computer or web browser associated with the **SUBJECT ACCOUNT** including the IP addresses, dates, and times associated with the recognition of any such cookie.
10. All records or other information regarding the identification of the **SUBJECT ACCOUNT**, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the **SUBJECT ACCOUNT** were created, devices associated with the account, the length of service, the IP address used to register the **SUBJECT ACCOUNT**, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
11. Any photos, documents, or other files that may indicate user attribution or ownership of the **SUBJECT ACCOUNT**;
12. The types of service utilized or associated with the **SUBJECT ACCOUNT**;
13. All records or other information stored at any time by an individual using the **SUBJECT ACCOUNT**, including address books, contact and buddy lists, calendar data, pictures, and files;
14. Any and all location data pertaining to the latitude and longitude of where the account was accessed;
15. All records and other information concerning any computer file created, stored, revised, or accessed in connection with the **SUBJECT ACCOUNT** or by a **SUBJECT ACCOUNT** user, including the contents and revision history of each document or other computer file, and all records and other information about each connection made to or from such document or other computer file, including the date, time, length, and method of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers;
16. For all information required to be disclosed pursuant to this warrant, the physical locations where the information is stored.

Google is hereby ordered to disclose the above information to the government within 10 days of receipt of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 1591– sex trafficking of a minor, involving the accounts of the user(s) of Google account identified on Attachment A, information pertaining to the following matters:

(a) Evidence indicating how and when the Google account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Google account owner;

(b) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(c) Location Data

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.